Analyse und Begründung von DMARC-Rejects

(Postfix + OpenDMARC 1.4.2)

1. Zweck

Diese SOP beschreibt, wie DMARC-Rejects auf dem Mailserver revisionssicher analysiert und begründet werden, ohne die betroffene E-Mail anzunehmen oder erneut senden zu lassen.

2. Systemkontext

- MTA: Postfix
- DMARC-Filter: OpenDMARC 1.4.2
- SPF-Prüfung: policyd-spf
- DKIM-Prüfung: OpenDKIM
- Entscheidungspunkt: SMTP END-OF-MESSAGE

3. Grundprinzip

OpenDMARC loggt nur das Endergebnis der DMARC-Evaluation, nicht die Detailursachen. Die Ursache eines Rejects wird durch Log-Korrelation ermittelt.

4. Relevante Logquellen

- Postfix (SMTP-Rejects)
- policyd-spf (SPF-Ergebnis, identity)
- OpenDMARC (pass/fail/none pro Domain)

5. Entscheidungslogik

DMARC besteht nur, wenn mindestens ein Mechanismus DMARC-konform erfolgreich ist: - SPF(mailfrom) aligned - DKIM valid + aligned

SPF über HELO ist für DMARC nicht verwertbar.

6. Ableitungsregel

Wenn SPF nur über HELO erfolgreich war und DMARC fail meldet, muss DKIM fehlgeschlagen sein.

7. Revisionssichere Begründung

Die E-Mail wurde gemäß der DMARC-Policy der Absenderdomain abgelehnt, da keine DMARC-konforme Authentifizierung vorlag.

8. Referenzen

RFC 7489 (DMARC), RFC 7208 (SPF), RFC 6376 (DKIM)